

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-190797

(P2002-190797A)

(43)公開日 平成14年7月5日(2002.7.5)

(51)Int.Cl.⁷

識別記号

F I

テーマコード*(参考)

H 0 4 L 9/10

G 0 6 F 12/14

G 0 9 C 1/00

H 0 4 H 1/00

3 2 0

6 6 0

G 0 6 F 12/14

G 0 9 C 1/00

H 0 4 H 1/00

H 0 4 L 9/00

3 2 0 B 5 B 0 1 7

3 2 0 F 5 J 1 0 4

6 6 0 E

F

6 2 1 A

審査請求 未請求 請求項の数12 O L (全 16 頁) 最終頁に続く

(21)出願番号

特願2001-311039(P2001-311039)

(62)分割の表示

特願平9-181186の分割

(22)出願日

平成9年7月7日(1997.7.7)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 伊藤 浩道

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72)発明者 荒井 正人

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74)代理人 100084032

弁理士 三品 岩男 (外1名)

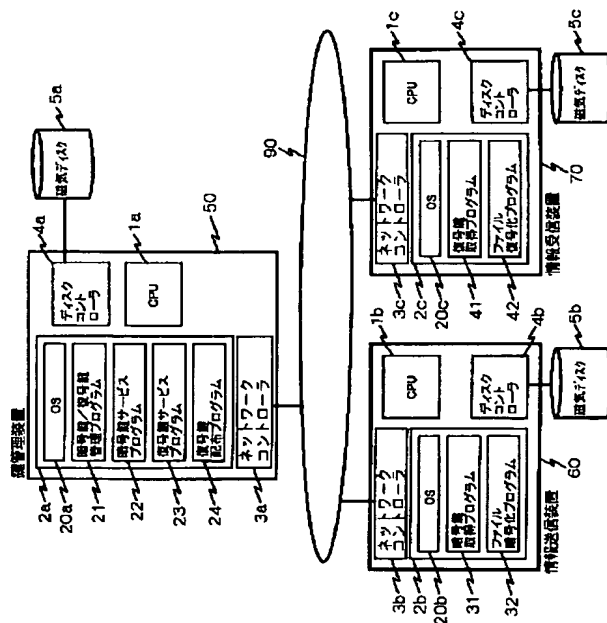
最終頁に続く

(54)【発明の名称】 鍵管理システム、鍵管理装置、情報暗号化装置、情報復号化装置、およびプログラムを記憶した記憶媒体

(57)【要約】

【課題】情報の同時公開を実現するのに好適なシステムを提供する。

【解決手段】鍵管理装置50は、復号鍵とその公開日時との対応関係を示す管理テーブルを参照して情報送信装置60が要求した日時に対応する復号鍵と対の暗号鍵を検索し、これを情報送信装置60に送信する。また、管理テーブルにしたがい、現在の日時に対応する復号鍵を公開する。情報送信装置60は、情報の機密性が解除される日時を鍵管理装置50に送信する。そして、鍵管理装置50から送られてきた暗号鍵を用いて情報を暗号化し、この暗号化された情報に当該情報についての日時を付与して情報受信装置70に送信する。情報受信装置70は、受け取った暗号化情報に付与された日時になったときに鍵管理装置50で公開されている復号鍵を取得し、この復号鍵を用いて暗号化情報を復号化する。



【特許請求の範囲】

【請求項 1】暗号鍵を用いて情報を暗号化する情報暗号化装置と、復号鍵を用いて情報を復号化する情報復号化装置と、前記情報暗号化装置および前記情報復号化装置で用いる暗号鍵および復号鍵を管理する鍵管理装置とを備え、少なくとも前記情報暗号化装置および前記鍵管理装置間が通信ネットワークで接続された鍵管理システムであって、

前記鍵管理装置は、

少なくとも 1 組の暗号鍵および復号鍵を記憶する鍵記憶手段と、

前記記憶手段に記憶された復号鍵と、当該復号鍵の公開日あるいは公開日時と、の対応関係を示す管理テーブルを記憶する管理テーブル記憶手段と、

前記管理テーブル記憶手段に記憶された管理テーブルを参照することで、前記情報暗号化装置が要求した日あるいは日時に対応する復号鍵と対の暗号鍵を検索する鍵検索手段と、

前記検索手段で検索した暗号鍵を、通信ネットワークを介して前記情報暗号化装置に送信する暗号鍵送信手段と、

前記管理テーブル記憶手段に記憶された管理テーブルにしたがい、現在の日あるいは日時に対応する復号鍵を公開する復号鍵公開手段と、を備えており、

前記情報暗号化装置は、

暗号化すべき情報の機密性が解除される日あるいは日時に関する日時情報を、通信ネットワークを介して前記鍵管理装置に送信する日時情報送信手段と、

通信ネットワークを介して前記鍵管理装置から送られてきた、前記日時情報送信手段が送信した日時情報で特定される日あるいは日時に対応する暗号鍵を受信する暗号鍵受信手段と、

前記暗号鍵受信手段で受信した暗号鍵を用いて、情報を暗号化する暗号化手段と、

前記暗号化手段で暗号化された情報に当該情報についての前記日時情報を付与して、前記情報復号化装置に配布する暗号化情報を作成する暗号化情報作成手段と、を備えており、

前記情報復号化装置は、

前記情報暗号化装置によって作成された暗号化情報を取得する暗号化情報取得手段と、

前記暗号化情報取得手段で取得した暗号化情報に付与された日時情報で特定される日あるいは日時になったときに、前記鍵管理装置で公開されている復号鍵を取得する復号鍵取得手段と、

前記復号鍵取得手段で取得した復号鍵を用いて、前記暗号化情報取得手段で取得した暗号化情報を復号化する復号化手段と、を備えていることを特徴とする鍵管理システム。

【請求項 2】請求項 1 記載の鍵管理システムであって、

前記情報復号化装置は複数あり、当該複数の情報復号化装置各々と前記鍵管理装置とは通信ネットワークを介して接続されており、

前記鍵管理装置の復号鍵公開手段は、前記複数の情報復号化装置を宛先とするブロードキャストパケットあるいはマルチキャストパケットにより、復号鍵を、通信ネットワークを介して前記複数の情報復号化装置に一斉同報通信するものであることを特徴とする鍵管理システム。

【請求項 3】請求項 1 記載の鍵管理システムであって、

前記情報復号化装置は複数あり、

前記鍵管理装置の復号鍵公開手段は、無線放送を利用することで、前記複数の情報復号化装置に対して復号鍵の公開を行うものであることを特徴とする鍵管理システム。

【請求項 4】請求項 1、2 または 3 記載の鍵管理システムであって、

前記鍵管理装置は、前記情報暗号化装置が要求した日あるいは日時に対応する復号鍵が前記管理テーブル記憶手段に記憶された管理テーブルにない場合に、新たに 1 組の暗号鍵および復号鍵を生成する鍵生成手段と、

前記鍵生成手段で生成した暗号鍵および復号鍵に、前記情報暗号化装置が要求した日あるいは日時を対応付けて、前記管理テーブルに追加する管理テーブル作成手段と、をさらに備えていることを特徴とする鍵管理システム。

【請求項 5】請求項 1、2、3 または 4 記載の鍵管理システムであって、

前記情報暗号化装置において、

前記暗号化手段は、送信すべき情報をデータ鍵を用いて暗号化するとともに、当該データ鍵を、操作者によって入力された個別暗号鍵および前記暗号鍵受信手段で受信した暗号鍵を用いて二重に暗号化するものであり、

前記情報作成手段は、前記暗号化手段で暗号化された情報に、当該情報についての前記日時情報および前記暗号化手段で二重に暗号化されたデータ鍵を付与して、前記情報復号化装置に配布する暗号化情報を作成するものであり、

前記情報復号化装置において、

前記復号化手段は、操作者によって入力された前記個別暗号鍵および前記復号鍵取得手段で取得した復号鍵を用いて、前記暗号化情報取得手段で取得した暗号化情報に付加された、二重に暗号化されたデータ鍵を復号化するとともに、当該復号化されたデータ鍵を用いて暗号化情報を復号化するものであることを特徴とする鍵管理システム。

【請求項 6】請求項 1、2、3、4 または 5 記載の鍵管理システムであって、

前記情報暗号化装置および前記情報復号化装置間は、通信ネットワークを介して接続されており、

前記情報暗号化装置は、前記暗号化情報作成手段で作成

10

20

30

40

50

3

した暗号化情報を通信ネットワークを介して前記情報復号化装置に送信する暗号化情報送信手段をさらに備えていることを特徴とする鍵管理システム。

【請求項7】情報の暗号化および復号化に使用する暗号鍵および復号鍵を管理する鍵管理装置であって、少なくとも1組の暗号鍵および復号鍵を記憶する鍵記憶手段と、

前記記憶手段に記憶された復号鍵と、当該復号鍵の公開日あるいは公開日時と、の対応関係を示す管理テーブルを記憶する管理テーブル記憶手段と、

前記管理テーブル記憶手段に記憶された管理テーブルを参照することで、情報の暗号化を行う情報暗号化装置が要求した日あるいは日時に対応する復号鍵と対の暗号鍵を検索する鍵検索手段と、

前記検索手段で検索した暗号鍵を前記情報暗号化装置に送信する暗号鍵送信手段と、

前記管理テーブル記憶手段に記憶された管理テーブルにしたがい、現在の日あるいは日時に対応する復号鍵を、情報の復号化を行う少なくとも1つ情報復号化装置に公開する復号鍵公開手段と、

を備えていることを特徴とする鍵管理装置。

【請求項8】情報の暗号化を行う情報暗号化装置であって、

暗号鍵および復号鍵の管理を行う鍵管理装置から、当該鍵管理装置において、暗号化すべき情報の機密性が解除される日あるいは日時に公開される復号鍵と対の暗号鍵を取得する暗号鍵取得手段と、

前記暗号鍵取得手段で取得した暗号鍵を用いて、情報を暗号化する暗号化手段と、

前記暗号化手段で暗号化された情報に、当該情報についての機密性が解除される日あるいは日時に関する情報を付与することで、当該情報の復号化を行う情報復号化装置に配布する暗号化情報を作成する暗号化情報作成手段と、

を備えていることを特徴とする情報暗号化装置。

【請求項9】情報の復号化を行う情報復号化装置であって、

当該情報復号化装置は、請求項8記載の情報暗号化装置で作成された暗号化情報を復号化するものであり、

請求項8記載の情報暗号化装置で作成された暗号化情報に付与された、当該暗号化情報の機密性が解除される日あるいは日時に関する情報を取得する日時情報取得手段と、

現在の日あるいは日時が前記日時情報取得手段で取得した情報で特定される日あるいは日時となったときに、請求項8記載の鍵管理装置において公開されている復号鍵を取得する復号鍵取得手段と、

前記復号鍵取得手段で取得した復号鍵を用いて、請求項8記載の情報暗号化装置で作成された暗号化情報を復号化する復号化手段と、

4

を備えていることを特徴とする情報復号化装置。

【請求項10】情報の暗号化および復号化に使用する暗号鍵および復号鍵を管理するためのプログラムを記憶した記憶媒体であって、

当該プログラムは、情報処理装置に、

少なくとも1組の暗号鍵および復号鍵を、当該復号鍵の公開日あるいは公開日時に対応付けて、これを管理テーブルとして、記憶装置に記憶させる第一の処理と、

10 前記記憶装置に記憶された管理テーブルを参照することで、情報の暗号化を行う情報暗号化装置が要求した日あるいは日時に対応する復号鍵と対の暗号鍵を検索する第二の処理と、

前記第二の処理で検索した暗号鍵を前記情報暗号化装置に送信する第三の処理と、

前記記憶装置に記憶された管理テーブルにしたがい、現在の日あるいは日時に対応する復号鍵を、情報の復号化を行う少なくとも1つ情報復号化装置に公開する第四の処理と、を実行させるものであることを特徴とするプログラムを記憶した記憶媒体。

20 【請求項11】情報の暗号化を行うためのプログラムを記憶した記録媒体であって、

当該プログラムは、情報処理装置に、

暗号鍵および復号鍵の管理を行う鍵管理装置から、当該鍵管理装置において、暗号化すべき情報の機密性が解除される日あるいは日時に公開される復号鍵と対の暗号鍵を取得する第一の処理と、

前記第一の処理で取得した暗号鍵を用いて、情報を暗号化する第二の処理と、

30 前記第二の処理で暗号化された情報に、当該情報についての機密性が解除される日あるいは日時に関する情報を付与することで、当該情報の復号化を行う情報復号化装置に配布する暗号化情報を作成する第三の処理と、を実行させるものであることを特徴とするプログラムを記憶した記憶媒体。

【請求項12】情報の復号化を行うプログラムを記憶した記憶媒体であって、

当該プログラムは、請求項11記載の記憶媒体に記憶されたプログラムを実行した情報処理装置で作成された暗号化情報を復号化するためのものであり、

40 情報処理装置に、

請求項11記載の記憶媒体に記憶されたプログラムを実行した情報処理装置で作成された暗号化情報に付与された、当該暗号化情報の機密性が解除される日あるいは日時に関する情報を取得する第四の処理と、

現在の日あるいは日時が前記第四の処理で取得した情報で特定される日あるいは日時となったときに、請求項11記載の鍵管理装置において公開されている復号鍵を取得する第五の処理と、

50 前記第五の処理で取得した復号鍵を用いて、請求項11記載の記憶媒体に記憶されたプログラムを実行した情報

処理装置で作成された暗号化情報を復号化する第六の処理と、を実行させるものであることを特徴とするプログラムを記憶した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号データを復号する復号鍵を管理するためのシステムに関し、特に、通信ネットワーク上で、複数のユーザに対する情報の同時公開を実現するのに好適なシステムに関する。

【0002】

【従来の技術】近年、インターネットなどの通信ネットワークを介して、複数の端末間での情報のやり取りが盛んに行われている。

【0003】ところで、通信ネットワークを介してやり取りされる情報のなかには、ある日時以前は秘密にしておく必要があるが、その後は開示しても構わないといった性質を有するものがある。たとえば、政府の機密情報などである。また、情報の開示が、複数の利用者に対して同時に行われていること（言い換えれば、複数の利用者が、情報の中身を同時に知ることができる状態にすること）を保証しなければならないものもある。たとえば、入札など商取引に関する情報などである。

【0004】このような情報に対して、従来は、情報作成者側の端末において、作成した情報を当該情報の機密性が解除される日あるいは日時まで保持し、機密性が解除されたときに、すなわち機密期限が切れたときに、はじめて、複数の利用者へ公開あるいは配布する方法が利用されている。

【0005】

【発明が解決しようとする課題】しかしながら、上記の方法では、情報作成者は、公開あるいは配布すべき情報の量が膨大である場合や、配布対象となる利用者の数が多い場合、複数の利用者に対し情報を、同時にしかも確実に開示することが容易でない。

【0006】また、情報作成者は、当該情報の公開あるいは配布日時を管理しなければならない。特に、複数種の情報を開示あるいは配布する場合において、これ等の情報の開示あるいは配布の日時が重なった場合、複数の利用者に対し情報の公開あるいは配布の同時性を保証することが困難である。

【0007】本発明は上記事情に鑑みてなされたものであり、本発明の目的は、複数のユーザに対する情報の同時公開を実現するのに好適なシステムを提供する。

【0008】

【課題を解決するための手段】本発明は、ネットワーク上を伝送される情報のセキュリティを確保する技術である鍵暗号方式を利用することで、上記課題を解決している。

【0009】具体的には、暗号鍵を用いて情報を暗号化する情報暗号化装置と、復号鍵を用いて情報を復号化する

る情報復号化装置と、前記情報暗号化装置および前記情報復号化装置で用いる暗号鍵および復号鍵を管理する鍵管理装置とを備え、少なくとも前記情報暗号化装置および前記鍵管理装置間が通信ネットワークで接続された鍵管理システムであって、前記鍵管理装置は、少なくとも1組の暗号鍵および復号鍵を記憶する鍵記憶手段と、前記記憶手段に記憶された復号鍵と、当該復号鍵の公開日あるいは公開日時と、の対応関係を示す管理テーブルを記憶する管理テーブル記憶手段と、前記管理テーブル記憶手段に記憶された管理テーブルを参照することで、前記情報暗号化装置が要求した日あるいは日時に対応する復号鍵と対の暗号鍵を検索する鍵検索手段と、前記検索手段で検索した暗号鍵を、通信ネットワークを介して前記情報暗号化装置に送信する暗号鍵送信手段と、前記管理テーブル記憶手段に記憶された管理テーブルにしたがい、現在の日あるいは日時に対応する復号鍵を公開する復号鍵公開手段と、を備えており、前記情報暗号化装置は、暗号化すべき情報の機密性が解除される日あるいは日時に関する日時情報を、通信ネットワークを介して前記鍵管理装置に送信する日時情報送信手段と、通信ネットワークを介して前記鍵管理装置から送られてきた、前記日時情報送信手段が送信した日時情報で特定される日あるいは日時に対応する暗号鍵を受信する暗号鍵受信手段と、前記暗号鍵受信手段で受信した暗号鍵を用いて、情報を暗号化する暗号化手段と、前記暗号化手段で暗号化された情報に当該情報についての前記日時情報を付与して、前記情報復号化装置に配布する暗号化情報を作成する暗号化情報作成手段と、を備えており、前記情報復号化装置は、前記情報暗号化装置によって作成された暗号化情報を取得する暗号化情報取得手段と、前記暗号化情報取得手段で取得した暗号化情報に付与された日時情報で特定される日あるいは日時になったときに、前記鍵管理装置で公開されている復号鍵を取得する復号鍵取得手段と、前記復号鍵取得手段で取得した復号鍵を用いて、前記暗号化情報取得手段で取得した暗号化情報を復号化する復号化手段と、を備えている。

【0010】ここで、暗号鍵および復号鍵とは、たとえば、公開鍵暗号方式における公開鍵および秘密鍵である。

【0011】本発明は、前記の構成により、情報作成者は、作成した情報を、当該情報の機密性が解除される日あるいは日時以前に、当該情報を暗号化して利用者へ配布することができる。したがって、情報作成者は、作成した情報の公開日時を管理する必要がなくなる。

【0012】また、情報の利用者は、受け取った暗号化情報の機密性が解除される日あるいは日時になるまで、当該情報を復号化するための復号鍵を取得することができない。したがって、その日あるいは日時まで情報を機密にすることができる。

【0013】さらに、情報の利用者は、受け取った情報

の機密性が解除される日あるいは日時以降は、当該情報を復号化するための復号鍵を取得することができる。したがって、当該復号鍵を用いて予め受け取った暗号化情報を復号化することにより、複数の利用者に対して、情報公開の同時性を保証することができる。

【0014】なお、本発明において、前記情報復号化装置が複数ある場合、当該複数の情報復号化装置各々と前記鍵管理装置とを通信ネットワークを介して接続し、前記鍵管理装置の復号鍵公開手段が、前記複数の情報復号化装置を宛先とするブロードキャストパケットあるいはマルチキャストパケットにより、復号鍵を、通信ネットワークを介して前記複数の情報復号化装置に一斉同報通信するようにしてもよい。あるいは、当該複数の情報復号化装置各々と前記鍵管理装置とを通信ネットワークを介して接続することなく、前記鍵管理装置の復号鍵公開手段が、無線放送を利用することで、前記複数の情報復号化装置に対して復号鍵の公開を行うようにしてもよい。

【0015】また、本発明において、前記鍵管理装置に、前記情報暗号化装置が要求した日あるいは日時に対応する復号鍵が前記管理テーブル記憶手段に記憶された管理テーブルにない場合に、新たに1組の暗号鍵および復号鍵を生成する鍵生成手段と、前記鍵生成手段で生成した暗号鍵および復号鍵に、前記情報暗号化装置が要求した日あるいは日時を対応付けて、前記管理テーブルに追加する管理テーブル作成手段と、をさらに備えてもよい。

【0016】

【発明の実施の形態】以下に、本発明の一実施形態について説明する。

【0017】図1は、本実施形態が適用された鍵管理システムの全体構成を示す図である。

【0018】ここで、符号50は鍵管理装置、符号60は情報送信装置、符号70は情報受信装置である。これ等の装置は、LANなどの通信ネットワーク90を介して互いに接続されている。

【0019】なお、ここでは、情報送信装置60および情報受信装置70を各々1つ示しているが、これに限定されるものではなく、各々複数あってもよい。

【0020】図1に示す各装置50、60、70は、通信機能を備えた情報処理装置、たとえばパーソナルコンピュータを用いることで、実現可能である。

【0021】鍵管理装置50は、情報暗号処理に用いる暗号鍵および情報復号処理に用いる復号鍵の管理を行う機能を有する。この機能は、CPU1aが、ディスクコントローラ4aを介して磁気ディスク5aからメモリ2a上にロードされた暗号鍵／復号鍵管理プログラム21、暗号鍵サービスプログラム22、復号鍵サービスプログラム23、および復号鍵配布プログラム24を実行することで実現される。なお、図1において、符号20

aはオペレーティングシステム(OS)、符号3aは、ネットワーク90を介した通信を実現するためのネットワークコントローラである。

【0022】磁気ディスク5aには、上記のOS20a、暗号鍵／復号鍵管理プログラム21、暗号鍵サービスプログラム22、復号鍵サービスプログラム23、および復号鍵配布プログラム24の他、少なくとも1組の暗号鍵および復号鍵が記憶されている。この少なくとも1組の暗号鍵および復号鍵は、各々当該復号鍵の公開日時と対応付けられて、鍵管理テーブル100として記憶される。

【0023】鍵管理テーブル100の一例を図2に示す。この例では、磁気ディスク5aに記憶されている複数の暗号鍵102および復号鍵103が、各々復号鍵103の公開日時である日付時刻101に対応付けられている。

【0024】ここで、暗号鍵102および復号鍵103は、公開鍵暗号方式における公開鍵および秘密鍵である。公開鍵暗号方式における公開鍵および秘密鍵は、いずれか一方から他方を求めることが極めて困難であるといった性質を有する。そこで、公開鍵暗号方式では、暗号化用の公開鍵を秘密にせず公開しておき、復号用の秘密鍵のみを秘密にしておく。すなわち、公開されている公開鍵を取得することで、誰でも情報の暗号化を行うことができるが、当該公開鍵で暗号化された情報の復号化については、当該公開鍵と対の秘密鍵を所有する者のみが行うことができるようにすることで、ネットワーク上を伝送される情報のセキュリティを確保している。

【0025】公開鍵暗号方式における公開鍵および秘密鍵は、初期値から結果の値を求めることは容易でも、結果の値から初期値を求めることは極めて困難な方向性関数を用いて実現されている。ここでは、現在広く用いられているRSA(Rivest, Shamir, Adleman)と呼ばれるシステムについて簡単に説明する。

【0026】まず、二つの大きな素数 p 、 q を用意する。そして、 p と q との積 pq を n とする。次に、 n のオイラー関数

$$\phi(n) = (p-1)(q-1)$$

に関し、互いに素である任意の数 e を選ぶ。そして、 $\phi(n)$ のモジュロの基での e の逆数

$$ed = 1 \bmod \phi(n)$$

となる数 d を求める。すると、平文 M 、暗号文 C に関し、

$$C = (M^e) \bmod n$$

$$M = (C^d) \bmod n$$

が成り立つことが証明される。したがって、 d を秘密鍵とし、 e と n の組を公開鍵とすることができる。図2における $e112$ および $n122$ は、上記の式における e 、 n に相当する。

【0027】公開鍵暗号化方式については、たとえば

「データ保護と暗号化の研究、一松信監修、日本経済新聞社（昭58）」などで詳しく述べられている。

【0028】情報送信装置60は、情報の暗号化を行う機能を有する。この機能は、CPU1bが、ディスクコントローラ4bを介して磁気ディスク5bからメモリ2b上にロードされた暗号鍵取得プログラム31およびファイル暗号化プログラム32を実行することで実現される。なお、図1において、符号20bはOS、符号3bは、通信ネットワーク90を介した通信を実現するためのネットワークコントローラである。

【0029】情報受信装置70は、情報の復号化を行う機能を有する。この機能は、CPU1cが、ディスクコントローラ4cを介して磁気ディスク5cからメモリ2c上にロードされた復号鍵取得プログラム41およびファイル復号化プログラム42を実行することで実現される。なお、図1において、符号20cはOS、符号3cは、通信ネットワーク90を介した通信を実現するためのネットワークコントローラである。

【0030】上記構成の鍵管理システムの動作について簡単に説明する。

【0031】まず、情報送信装置60は、暗号化すべき情報の機密性が解除される日時に関する情報を、通信ネットワーク90を介して鍵管理装置50へ送信する。

【0032】これを受けて、鍵管理装置50は、磁気ディスク5aに記憶されている鍵管理テーブル100を参照することで、情報送信装置60から送られてきた情報によって特定される日時に対応する暗号鍵を検索する。そして、検索した暗号鍵を、通信ネットワーク90を介して、情報送信装置60へ送信する。

【0033】また、鍵管理装置50は、磁気ディスク5aに記憶されている鍵管理テーブル100にしたがい、現在の日時に対応する復号鍵を順次読み出して公開する。

【0034】情報送信装置60は、鍵管理装置50から送られてきた暗号鍵を用いて、情報受信装置70へ送信する情報を暗号化する。そして、暗号化した情報（以下、暗号化情報ともいう）に、当該情報の機密性が解除される日時に関する情報を付加して、情報受信装置60へ、通信ネットワーク90を介して送信する。

【0035】これを受けて、情報受信装置70は、現在の日時が、情報送信装置60から送られてきた暗号化情報に付与された日時に関する情報で特定される日時になるまで待ち、当該日時となったときに、鍵管理装置50で公開されている復号鍵を取得する。そして、取得した復号鍵で、情報送信装置60から送られてきた暗号化情報を復号化する。

【0036】次に、本実施形態システムを構成する各装置の詳細について説明する。

【0037】まず、鍵管理装置50の詳細について説明する。

【0038】最初に、鍵管理装置50において、CPU1aがメモリ2a上にロードされた暗号鍵／復号鍵管理プログラム21を実行した場合の動作について説明する。

【0039】図3は、鍵管理装置50において、CPU1aがメモリ2a上にロードされた暗号鍵／復号鍵管理プログラム21を実行した場合の動作を説明するためのフロー図である。

10 【0040】まず、図示していない表示装置などを用いて、鍵管理装置50のオペレータに対して、鍵管理テーブル100に追加する鍵を特定するための情報である、開始日時、終了日時、および時間間隔を入力するように促す。これを受けて、ステップ601～603において、図示していない入力装置に入力された開始日時、終了日時、および時間間隔を受け付ける。

【0041】ステップ604では、暗号鍵／復号鍵生成ルーチンを呼び出して、一組の暗号鍵（e，n）および復号鍵（d）を生成する。この暗号鍵／復号鍵生成ルーチンについては後述する。

20 【0042】ステップ605では、鍵管理テーブル100に日付時刻を追加する。ここで、日付時刻とは、図3に示すフローにおいて、ステップ605での処理が一回目である場合は、ステップ601で受け付けた開始日時、二回目以降の場合は、後述するステップ609で算出した日付時刻である。

【0043】ステップ606では、ステップ604で生成した暗号鍵（e，n）を、鍵管理テーブル100の、ステップ605で当該鍵管理テーブル100に追加した日付時刻に対応する欄に追加する。

30 【0044】ステップ607では、ステップ604で生成した復号鍵（d）を、鍵管理テーブル100の、ステップ605で当該鍵管理テーブル100に追加した日付時刻に対応する欄に追加する。

【0045】ステップ608では、ステップ605で鍵管理テーブル100に追加した日付時刻が、ステップ602で受け付けた終了日時以降の日時となったか否かを判断する。終了日時以降の日時となっていない場合は、ステップ609へ移行して、ステップ605で鍵管理テーブル100に追加した日付時刻に、ステップ603で受け付けた日時間間隔を加算し、得られた結果を新たな日付時刻に設定する。

【0046】一方、終了日時以降の日時となっている場合は、このフローを終了する。

【0047】上記のフローにより、CPU1aは、暗号鍵／復号鍵管理プログラム21を実行することで、図2に示すような、公開鍵及び復号鍵と、復号鍵を公開する日付時刻と、を対応付けた鍵管理テーブル100を作成することができる。

50 【0048】次に、図3に示すフローのステップ604での処理（暗号鍵／復号鍵生成ルーチン）について説明

する。

【0049】図4は、鍵管理装置50において、CPU1aがメモリ2a上にロードされた暗号鍵／復号鍵管理プログラム21のうちの暗号鍵／復号鍵生成ルーチン700を実行した場合の動作を説明するためのフロー図である。

【0050】まず、二つの大きな素数p、qを生成し（ステップ701）、その後、この生成したpとqとの積 $n (=pq)$ を生成する（ステップ702）。

【0051】次に、この積 n のオイラー関数 $\phi(n) = (p-1)(q-1)$ に関し、互いに素である任意の数eを選択する（ステップ703）。そして、 $\phi(n)$ のモジュロの基でのeの逆数

$$ed = 1 \bmod \phi(n)$$

となる数dを求める（ステップ704）。次に、上記のステップ702～704で得たe、n、dを、戻り値として設定し（ステップ705）、その後、呼び出し元にリターンする（ステップ799）。

【0052】次に、鍵管理装置50において、CPU1aがメモリ2a上にロードされた暗号鍵サービスプログラム22を実行した場合の動作について説明する。

【0053】図5は、鍵管理装置50において、CPU1aがメモリ2a上にロードされた暗号鍵サービスプログラム22を実行した場合の動作を説明するためのフロー図である。なお、暗号鍵サービスプログラム22は、鍵管理装置50の常駐プログラムとして動作する。

【0054】まず、暗号鍵要求が通信ネットワーク90経由で送られてくるのを待つ（ステップ801）。暗号鍵要求を受信すると、当該要求元から送られてくる日時に関する情報を取得する（ステップ802）。

【0055】次に、ステップ802で取得した情報で特定される日時が、磁気ディスク5aに記憶された鍵管理テーブル100に存在するかどうかを調べる（ステップ803）。存在しない場合は、暗号鍵／復号鍵管理プログラム21を呼び出し、ステップ802で取得した情報で特定される日時を図3のステップ601、602で受け付ける開始日時および終了日時に設定し、図3のステップ603で受け付ける日時間隔を適当な時間に設定して、当該プログラムを実行する（ステップ804）。これにより、当該日時に対応付けられた暗号鍵および公開鍵が鍵管理テーブル100に追加される。ステップ804での処理を完了した後、ステップ805へ移行する。

【0056】一方、ステップ802で取得した情報で特定される日時が鍵管理テーブル100に存在する場合は、ステップ804を実行することなく、ステップ805へ移行する。

【0057】ステップ805では、鍵管理テーブル100からステップ802で取得した情報で特定される日時に対応付けられた暗号鍵を取り出す。その後、取り出し

た暗号鍵を、暗号鍵の要求元に送信する（ステップ806）。以上の処理を行った後、ステップ801に戻り、再び、暗号鍵要求が通信ネットワーク90経由で送られてくるのを待つ。

【0058】次に、鍵管理装置50において、CPU1aがメモリ2a上にロードされた復号鍵サービスプログラム23を実行した場合の動作について説明する。

【0059】図6は、鍵管理装置50において、CPU1aがメモリ2a上にロードされた復号鍵サービスプログラム23を実行した場合の動作を説明するためのフロー図である。なお、復号鍵サービスプログラム23は、鍵管理装置50の常駐プログラムとして動作する。

【0060】まず、復号鍵要求が通信ネットワーク90経由で送られてくるのを待つ（ステップ901）。復号鍵要求を受信すると、当該要求元から送られてくる日時に関する情報を取得する（ステップ902）。

【0061】次に、ステップ902で取得した情報で特定される日時が、磁気ディスク5aに記憶された鍵管理テーブル100に存在するかどうかを調べる（ステップ803）。存在しない場合は、復号鍵の要求元にエラーコードを送信し（ステップ906）、その後、ステップ901に戻り、再び、復号鍵要求が通信ネットワーク90経由で送られてくるのを待つ。

【0062】一方、ステップ902で取得した情報で特定される日時が鍵管理テーブル100に存在する場合、当該日時に対応付けられた復号鍵を取り出し（ステップ904）、取り出した復号鍵を、復号鍵の要求元に送信する（ステップ905）。その後、ステップ901に戻り、再び、復号鍵要求が通信ネットワーク90経由で送られてくるのを待つ。

【0063】次に、鍵管理装置50において、CPU1aがメモリ2a上にロードされた復号鍵配布プログラム24を実行した場合の動作について説明する。

【0064】図7は、鍵管理装置50において、CPU1aがメモリ2a上にロードされた復号鍵配布プログラム24を実行した場合の動作を説明するためのフロー図である。なお、復号鍵配布プログラム24は、鍵管理装置50の常駐プログラムとして動作する。

【0065】まず、OS20aが有する機能を利用して現在日時を取得し（ステップ1001）、その後、取得した現在日時に対応付けられた復号鍵を、鍵管理テーブル100から取り出す（ステップ1002）。

【0066】次に、鍵管理テーブル100から、ステップ1001で取得した日時の次の日時を検索する（ステップ1003）。そして、OS20aが有する機能を利用して取得した現在日時が、ステップ1003で検索した次の日時以降となったか否かを判断する（ステップ1004）。

【0067】次の日時以降となっていない場合は、ステップ1002で取得した復号鍵を、当該復号鍵に対応付

けられた日時に関する情報とともに、情報受信装置70（情報送信装置70が複数ある場合はその全て）に対して、通信ネットワーク90を介して一斉同報通信する（ステップ1005）。一斉同報通信は、通信ネットワークを用いた通信システムで利用されているブロードキャストパケットあるいはマルチキャストパケットを用いることで、実現可能である。ここで、ブロードキャストパケットとは、パケットのヘッダに、複数の宛先のアドレス各々を付与したものである。また、マルチキャストパケットとは、パケットのヘッダに、複数の宛先を示す1つのアドレスを付与したものである。

【0068】ステップ1005での処理を終了した後、OS20aが有する機能を利用して現在日時を取得し（ステップ1006）、ステップ1004へ戻る。

【0069】一方、ステップ1004において、次の日時以降となっている場合は、ステップ1002へ戻る。

【0070】上記のフローにより、鍵管理テーブル100に格納された複数の復号鍵各々は、自己に対応付けられた日時から次に公開すべき復号鍵に対応付けられた日時となるまで、繰り返し一斉同報通信される。ここで、上記のフローによって鍵管理装置50から送出される復号鍵の履歴の一例を図8に示す。

【0071】次に、情報送信装置60の詳細について説明する。

【0072】最初に、情報送信装置60で生成された暗号化情報の構成について説明する。

【0073】図9は、情報送信装置60で生成された暗号化情報の構成例を説明するための図である。なお、暗号化すべき情報は、データベースや電子メールなど電子的なデータならどのようなものでもよいが、ここでは、情報をファイル単位で暗号化した場合の例について示す。

【0074】図9において、符号202は、暗号化後の暗号文ファイルである。暗号文ファイル202は、平文ファイルを暗号化したデータである暗号文データ204と、暗号文データ204に付加されたヘッダ205と、から成る。

【0075】ヘッダ205には、復号が可能となる日時（すなわち、機密性が解除される日時）を示す情報である復号許可日時206と、暗号文データ204の元となる平文ファイルのファイル名207と、この平文ファイルのファイルサイズ208と、この平文ファイルの暗号化に用いたデータ鍵を、鍵管理装置50から取得した暗号鍵および後述する個別暗号鍵を用いて二重に暗号化したデータである二重暗号化データ鍵209と、で成る。

【0076】図9に示す暗号化情報の構成例から分かるように、本実施形態では、鍵管理装置50から取得した暗号鍵を用いて、平文ファイルを直接暗号化するのではなく、対称鍵暗号方式で用いられる鍵、すなわち暗号化および復号化の両方に共通して用いられるデータ鍵を用

いて、平文ファイルを暗号化するようにしている。そして、鍵管理装置50から取得した暗号鍵は、平文ファイルの暗号化に用いたデータ鍵を暗号化するのに用いている。

【0077】次に、情報送信装置60において、CPU1bがメモリ2b上にロードされたファイル暗号化プログラム32を実行した場合の動作について説明する。

【0078】図10は、情報送信装置60において、CPU1bがメモリ2b上にロードされたファイル暗号化プログラム32を実行した場合の動作を説明するためのフロー図である。

【0079】まず、図示していない表示装置などを用いて、情報送信装置60のユーザに対して、暗号化する平文のファイル名および当該ファイルの復号許可日時を入力するように促す。これを受けて、ステップ1101、1102において、図示していない入力装置に入力されたファイル名、および復号許可日時を受け付ける。

【0080】次に、ステップ1103において、ステップ1101で受け付けたファイル名で特定されるファイルをオープンにする。その後、仮の名称を付けた一時ファイルを作成する（ステップ1104）。

【0081】次に、ステップ1105では、データ鍵である乱数を生成する。その後、暗号鍵取得プログラム31を実行して、鍵管理装置50から、ステップ1102で受け付けた復号許可日時に公開される復号鍵と対の暗号鍵を取得する（ステップ1106）。

【0082】ステップ1107では、ステップ1105で生成したデータ鍵を、ステップ1106で鍵管理装置50から取得した暗号鍵を用いて暗号化して、暗号化データ鍵を生成する。その後、図示していない表示装置などを用いて、情報送信装置60のユーザに対して、ステップ1107で生成した暗号化データ鍵を二重に暗号化するための鍵である個別暗号鍵を入力するように促す。これを受けて、ステップ1108において、図示していない入力装置に入力された個別暗号鍵を受け付ける。

【0083】次に、ステップ1109では、ステップ1107で生成した暗号化データ鍵を、ステップ1108で受け付けた個別暗号鍵を用いて暗号化して、二重暗号化データ鍵を生成する。

【0084】ステップ1110では、ステップ1104で作成した一時ファイルの先頭部分にヘッダを付加する。そして、付加したヘッダに、ステップ1102で受け付けた復号許可日時を特定する情報、ステップ1101で受け付けたファイル名、このファイル名で特定されるファイルのサイズ、およびステップ1109で生成した二重暗号化データ鍵を、この順序で書き込む（ステップ1111）。

【0085】次に、ステップ1112では、ステップ1103でオープンにした平文ファイルからデータを読み出す。そして、読み出したデータを、ステップ1109

で生成した二重暗号化データ鍵を用いて暗号化して、暗号データを生成し（ステップ1113）、その後、この暗号データをステップ1104で作成した一時ファイルに書き込む（ステップ1114）。

【0086】ステップ1115では、ステップ1103でオープンにした平文ファイルの全データの暗号化が終了したか否かを判定する。終了していない場合は、終了するまで上記のステップ1112～ステップ1114を繰り返し実行する。そして、平文ファイルの全データの暗号化が終了した後、平文ファイルおよび一時ファイルの両方をクローズにする。

【0087】ステップ1117では、ステップ1101で受け付けた平文ファイルのファイル名と、ステップ1104で作成した一時ファイルの仮の名称とが同一であるか否かを判定する。同一である場合は、平文ファイルを削除し（ステップ1118）、その後、一時ファイルのファイル名を、ステップ1101で受け付けた平文ファイルのファイル名に変更する。そして、このフローを終了する。

【0088】一方、同一でない場合は、ステップ1104で作成した一時ファイルのファイル名を、ステップ1101で受け付けた平文ファイルのファイル名に変更して、このフローを終了する。

【0089】情報送信装置60は、上記のようにして作成した暗号文ファイルを、通信ネットワーク90を介して、所望の情報受信装置70に送信することができる。

【0090】次に、情報送信装置60において、CPU1bがメモリ2b上にロードされた暗号鍵取得プログラム31を実行した場合の動作について説明する。

【0091】図11は、情報送信装置60において、CPU1bがメモリ2b上にロードされた暗号鍵取得プログラム31を実行した場合の動作を説明するためのフロー図である。このフローは、図10に示すフローのステップ1106が行われることで、実行される。

【0092】まず、ステップ1301において、情報送信装置60を、通信ネットワーク90を介して、鍵管理装置50に接続する。

【0093】次に、ステップ1302において、図10に示すフローのステップ1102で受け付けた復号許可日時を特定する情報を、鍵管理装置50へ送信する。これを受けて、鍵管理装置50は、暗号鍵サービスプログラム22により、鍵管理テーブル100から復号許可日時に対応付けられた復号鍵を検索して、当該復号鍵を、復号許可日時を特定する情報を送信した情報送信装置60に送信する。

【0094】ステップ1303では、鍵管理装置50から送られてきた、ステップ1302で鍵管理装置に送信した復号許可日時に対応付けられた暗号鍵を受信する。次に、鍵管理装置50との接続を解除し（ステップ1304）、その後、ステップ1303で受信した暗号鍵を

戻り値に設定して（ステップ1305）、このフローを終了する。

【0095】次に、情報受信装置70の詳細について説明する。

【0096】最初に、情報受信装置70において、CPU1cがメモリ2c上にロードされたファイル復号化プログラム42を実行した場合の動作について説明する。

【0097】図12は、情報受信装置70において、CPU1cがメモリ2c上にロードされたファイル復号化プログラム42を実行した場合の動作を説明するためのフロー図である。

【0098】まず、図示していない表示装置などを用いて、情報受信装置70のユーザに対して、情報送信装置60から送られてきた暗号文ファイルのうち、復号しようとしている暗号文ファイルの名称を入力するように促す。これを受けて、ステップ1201において、図示していない入力装置に入力されたファイル名を受け付ける。

【0099】次に、ステップ1202において、ステップ1201で受け付けたファイル名で特定される暗号文ファイルをオープンにした後、この暗号文ファイルのヘッダから二重暗号化データ鍵を取り出す（ステップ1203）。その後、図示していない表示装置などを用いて、情報受信装置60のユーザに対して、取り出した二重暗号化データ鍵を復号化するのに用いる個別暗号鍵を入力するように促す。これを受けて、ステップ1204において、図示していない入力装置に入力された個別暗号鍵を受け付ける。

【0100】なお、個別暗号鍵は、暗号文ファイルの送信者から予め知らされているものとする。

【0101】次に、ステップ1205では、ステップ1203で取り出した二重暗号化データ鍵を、ステップ1204で受け付けた個別暗号鍵を用いて、一重の暗号化データ鍵に変換する。

【0102】ステップ1206では、ステップ1203でオープンにした暗号文ファイルのヘッダから復号許可日時に関する情報を取り出す。その後、この情報で特定される日時を引数として、復号鍵取得プログラム41を実行する（ステップ1207）。これにより、鍵管理装置50から、復号許可日時に対応付けられた復号鍵を取得する。

【0103】次に、ステップ1208では、ステップ1207で実行した復号鍵取得プログラム41からの戻り値を参照することで、復号鍵の取得に成功したか否かを判定する。取得に成功しなかった場合は、ステップ1202でオープンにした暗号文ファイルをクローズにし（ステップ1289）、このフローを終了する。

【0104】一方、復号鍵の取得に成功した場合は、ステップ1209に移行する。

【0105】ステップ1209では、ステップ1205

で得た一重の暗号化データ鍵を、ステップ1207で取得した復号鍵を用いて復号化することで、暗号文ファイルの暗号化に用いたデータ鍵を得る。

【0106】次に、ステップ1210では、仮の名称を付けた一時ファイルを作成する。その後、ステップ1202でオープンにした暗号文ファイルから暗号データを読み出す（ステップ1211）。そして、読み出した暗号データを、ステップ1209で生成したデータ鍵を用いて復号化して、平文データを生成し（ステップ1212）、その後、この平文データをステップ1210で作成した一時ファイルに書き込む（ステップ1213）。

【0107】ステップ1214では、ステップ1202でオープンにした暗号文ファイルの全暗号データの復号化が終了したか否かを判定する。終了していない場合は、終了するまで上記のステップ1211～ステップ1213を繰り返し実行する。そして、暗号文ファイルの全暗号データの復号化が終了した後、暗号文ファイルおよび一時ファイルの両方をクローズにする。

【0108】ステップ1216では、ステップ1201で受け付けた暗号文ファイルのファイル名と、ステップ1210で作成した一時ファイルの仮の名称とが同一であるか否かを判定する。同一である場合は、暗号文ファイルを削除し（ステップ12176）、その後、一時ファイルのファイル名を、ステップ1201で受け付けた暗号文ファイルのファイル名に変更する。そして、このフローを終了する。

【0109】一方、同一でない場合は、ステップ1210で作成した一時ファイルのファイル名を、ステップ1201で受け付けた暗号文ファイルのファイル名に変更して、このフローを終了する。

【0110】次に、情報受信装置70において、CPU1cがメモリ2c上にロードされた復号鍵取得プログラム41を実行した場合の動作について説明する。

【0111】図13は、情報受信装置70において、CPU1cがメモリ2c上にロードされた復号鍵取得プログラム41を実行した場合の動作を説明するためのフロー図である。このフローは、図12に示すフローのステップ1207が行われることで、実行される。

【0112】まず、ステップ1401において、OS20cが有する機能を利用して現在日時を取得する。次に、この取得した現在日時と、引数として受け取った復号許可日時とを比較する（ステップ1402）。この結果、現在日時が復号許可日時以降である場合はステップ1406に移行し、復号許可日時よりも前の日時である場合はステップ1403へ移行する。

【0113】ステップ1403では、図示していない表示装置などを用いて、情報受信装置70のユーザに対して、現在の日時が復号許可日時になるまで待機するか否かを問い合わせる。そして、図示していない入力装置に、ユーザに指示が入力されるのを待つ。

【0114】入力されたユーザの指示が、現在の日時が復号許可日時になるまで待機しないことを示す場合は、エラーコードを戻り値に設定し（ステップ1489）、その後、このフローを終了する。

【0115】一方、入力されたユーザの指示が、現在の日時が復号許可日時になるまで待機することを示す場合、OS20cが有する機能を利用して現在日時を取得し（ステップ1404）、その後、この取得した現在日時と、引数として受け取った復号許可日時とを比較する（ステップ1405）。このステップ1404およびステップ1405での処理を、取得した現在日時が、引数として受け取った復号許可日時以降となるまで、繰り返し実行する。

【0116】ステップ1406では、鍵管理装置50が公開している（通信ネットワーク90上を流れている）復号鍵を受信し、その中に、引数として受け取った復号許可日時に対応付けられた復号鍵があるか否かを判定する。この判定は、受信した復号鍵に付加されている日時に関する情報を基に行う。

【0117】引数として受け取った復号許可日時に対応付けられた復号鍵がある場合は、この復号鍵を戻り値に設定して（ステップ1479）、このフローを終了する。一方、引数として受け取った復号許可日時に対応付けられた復号鍵がない場合は、ステップ1408へ移行する。

【0118】ステップ1408では、情報受信装置70を、通信ネットワーク90を介して、鍵管理装置50に接続する。

【0119】次に、ステップ1409において、引数として受け取った復号許可日時を特定する情報を、鍵管理装置50へ送信する。これを受けて、鍵管理装置50は、復号鍵サービスプログラム23により、鍵管理テーブル100から復号許可日時に対応付けられた復号鍵を検索して、当該復号鍵を、復号許可日時を特定する情報を送信した情報受信装置70に送信する。

【0120】ステップ1410では、鍵管理装置50から送られてきた、復号許可日時に対応付けられた復号鍵を受信する。その後、鍵管理装置50との接続を解除する（ステップ1411）。次に、復号鍵の受信結果を調べて、復号鍵をエラーなく取得することができたか否かを判断する（ステップ1412）。

【0121】エラーなく取得することができた場合は、この取得した復号鍵を戻り値に設定して（ステップ1479）、このフローを終了する。一方、エラーがあり、取得に失敗した場合は、エラーコードを戻り値に設定し（ステップ1489）、その後、このフローを終了する。

【0122】上記説明した本実施形態の鍵管理システムでは、情報送信装置60のユーザは、作成した情報を、当該情報の機密性が解除される日時以前に、当該情報を

10

20

30

40

50

暗号化して利用者に配布することができる。したがって、作成した情報の公開日時を管理する必要がなくなる。

【0123】また、情報受信装置 70 のユーザは、受け取った暗号化情報の機密性が解除される日時になるまで、当該情報を復号化するための復号鍵を取得することができない。したがって、その日あるいは日時まで情報を機密にすることができる。

【0124】さらに、情報受信装置 70 のユーザは、受け取った情報の機密性が解除される日あるいは日時以降は、当該情報を復号化するための復号鍵を取得することができる。したがって、当該復号鍵を用いて予め受け取った暗号化情報を復号化することにより、複数の情報受信装置 70 のユーザに対して、情報公開の同時性を保証することができる。

【0125】なお、上記の実施形態では、鍵管理装置 50 での復号鍵の公開（一斉通報通信）を、図 8 に示すように 1 個のチャネルを用いて行うものについて説明した。しかしながら、本発明はこれに限定されるものではない。たとえば、図 14 に示すように、複数のチャネルを用いて、復号鍵の公開を行うようにしてもよい。この場合、同一の復号鍵の公開（一斉通報通信）期間を長くすることができる。これにより、情報受信装置 70 は、復号許可日時に達してからしばらく経った後でも、当該復号許可日時に対応する復号鍵を、鍵管理装置 50 にアクセスすることなく取得することが可能となる。

【0126】また、上記の実施形態では、鍵管理装置 50 において、鍵の公開を通信ネットワーク 90 を利用したブロードキャストパケットあるいはマルチキャストパケットにより行うものについて説明した。しかしながら、本発明は、これに限定されるものではない。復号鍵の公開は、図 15 に示すような衛星などを用いた無線放送によっても実現可能である。衛星などの無線放送を用いることで、複数の情報受信装置 70 全てに対して、同時に復号鍵を配布することが可能となる。

【0127】さらに、上記の実施形態では、個別暗号鍵でデータ鍵を暗号化する場合について説明したが、鍵管理装置 50 から取得する暗号鍵および復号鍵を、データの暗号化および復号化に直接用いることも可能である。ただし、この場合、復号許可日時が同一である暗号データは、この復号許可日時に対応付けられた復号鍵で全て復号できるという点に注意する必要がある。

【0128】くわえて、上記の実施形態では、情報送信装置 60 にて暗号化した情報を、通信ネットワークを介して情報受信装置 70 へ送信するものについて説明したが、暗号化した情報の配布は、通信ネットワークを介さずに、たとえば、フロッピー（登録商標）ディスクや CD-ROM などの記憶媒体に記録して行うようにしてもよい。また、上記の実施形態では、一台の鍵管理装置 50 を用いて、暗号鍵および復号鍵の管理やサービスなどを

行う場合について説明したが、これ等の処理を複数の情報処理装置に分担させるようにしてもよい。

【0129】また、上記の実施形態では、鍵管理システムを構成する各装置で実行される各種プログラムを、磁気ディスクに記憶させたものについて説明した。しかしながら、本発明はこれに限定されるものではなく、たとえば CD-ROM などの光ディスクやその他の記録媒体に記憶するようにしてもよい。

【0130】

10 【発明の効果】以上説明したように、本発明によれば、複数のユーザに対する情報の同時公開を実現するのに好適なシステムを提供することができる。

【図面の簡単な説明】

【図 1】本発明の一実施形態が適用された鍵管理システムの全体構成を示す図である。

【図 2】鍵管理装置 50 の磁気ディスク 5a に記憶されている鍵管理テーブル 100 の一例を示す図である。

20 【図 3】鍵管理装置 50 において、CPU 1a がメモリ 2a 上にロードされた暗号鍵／復号鍵管理プログラム 21 を実行した場合の動作を説明するためのフロー図である。本発明の実施例における暗号鍵管理システムの一構成例を示す図である。

【図 4】鍵管理装置 50 において、CPU 1a がメモリ 2a 上にロードされた暗号鍵／復号鍵管理プログラム 21 のうちの暗号鍵／復号鍵生成ルーチン 700 を実行した場合の動作を説明するためのフロー図である。

【図 5】鍵管理装置 50 において、CPU 1a がメモリ 2a 上にロードされた暗号鍵サービスプログラム 22 を実行した場合の動作を説明するためのフロー図である。

30 【図 6】鍵管理装置 50 において、CPU 1a がメモリ 2a 上にロードされた復号鍵サービスプログラム 23 を実行した場合の動作を説明するためのフロー図である。

【図 7】鍵管理装置 50 において、CPU 1a がメモリ 2a 上にロードされた復号鍵配布プログラム 24 を実行した場合の動作を説明するためのフロー図である。

【図 8】図 7 に示すフローによって鍵管理装置 50 から送出される復号鍵の履歴の一例を示す図である。

【図 9】情報送信装置 60 で生成された暗号化情報の構成例を説明するための図である。

40 【図 10】情報送信装置 60 において、CPU 1b がメモリ 2b 上にロードされたファイル暗号化プログラム 32 を実行した場合の動作を説明するためのフロー図である。

【図 11】情報送信装置 60 において、CPU 1b がメモリ 2b 上にロードされた暗号鍵取得プログラム 31 を実行した場合の動作を説明するためのフロー図である。

50 【図 12】情報受信装置 70 において、CPU 1c がメモリ 2c 上にロードされたファイル復号化プログラム 42 を実行した場合の動作を説明するためのフロー図である。

21

【図13】情報受信装置70において、CPU1cがメモリ2c上にロードされた復号鍵取得プログラム41を実行した場合の動作を説明するためのフロー図である。

【図14】本発明の一実施形態の変形例を説明するための図であり、複数のチャネルを用いて復号鍵の配布を行なった場合における、鍵管理装置50から送出される復号鍵の履歴の一例を示す図である。

【図15】本発明の一実施形態の変形例を説明するための図であり、復号鍵の配布に衛星などを用いた無線放送を用いた例を示す図である。

【符号の説明】

1a～1c CPU

2a～2c メモリ

3a～3c ネットワークコントローラ

4a～4c ディスクコントローラ

5a～5c 磁気ディスク

20a～20c OS

21 暗号鍵/復号鍵管理プログラム

22 暗号鍵サービスプログラム

23 復号鍵サービスプログラム

24 復号鍵配布プログラム

31 暗号鍵取得プログラム

32 ファイル暗号化プログラム

10 41 復号鍵取得プログラム

42 ファイル復号化プログラム

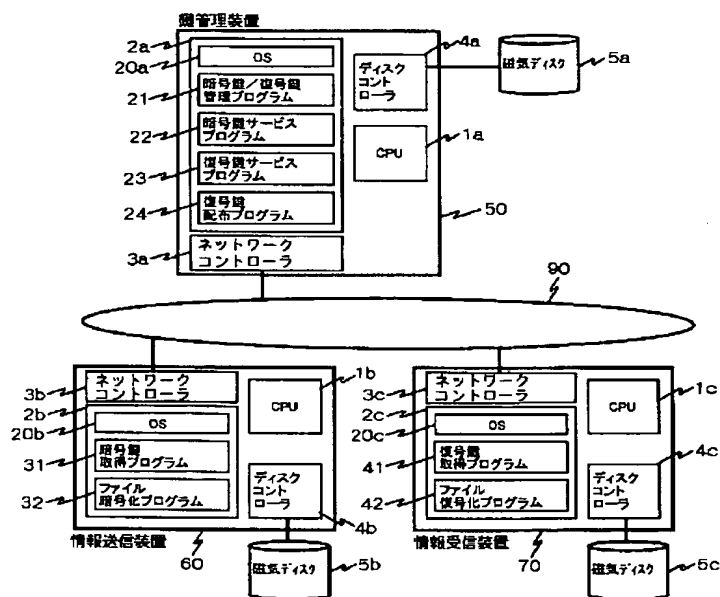
50 鍵管理装置

60 情報送信装置

70 情報受信装置

【図1】

図1



【図2】

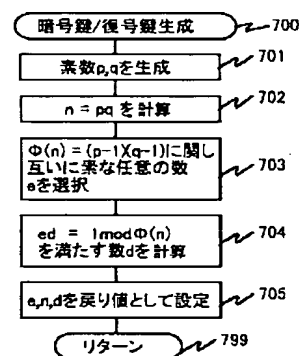
図2

日付時刻	暗号鍵 e	n	復号鍵 d
199701010000	8F04	1AB3B...F3CB	F7C3B...935B
199701010100	169B	D5499...1C86	6056D...7E9C
199701010200	EE7C	C869B...5FC8	413A6...F103
199912312100	8BD7	B1800...912F	36A9B...DF83
199912312200	A29F	AB39B...55FD	D0923...14F3
199912312300	4623	08469...EC01	CC08E...9FCB

鍵管理テーブル

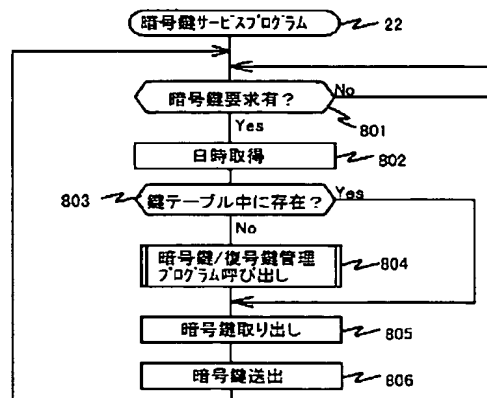
【図4】

図4



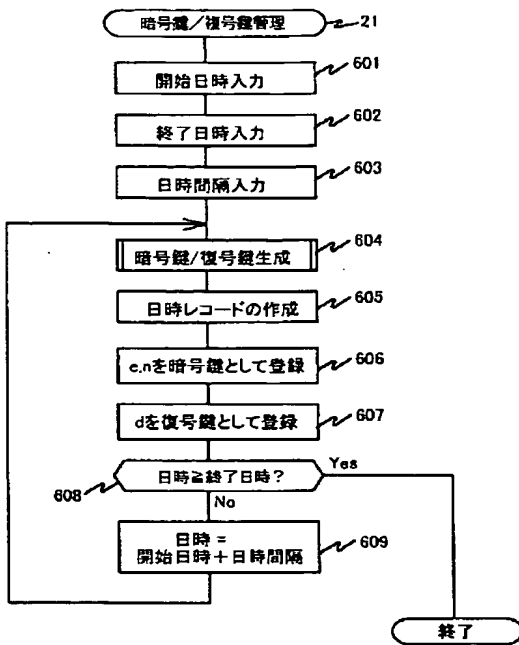
【図5】

図5



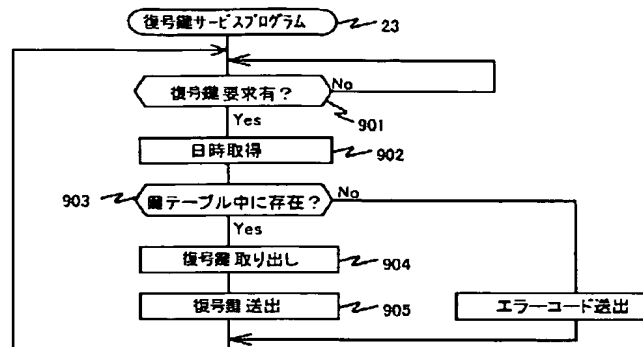
【図3】

図3



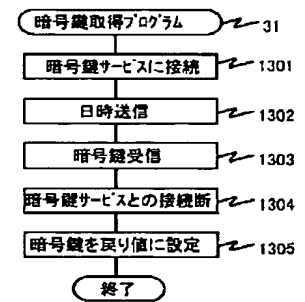
【図6】

図6



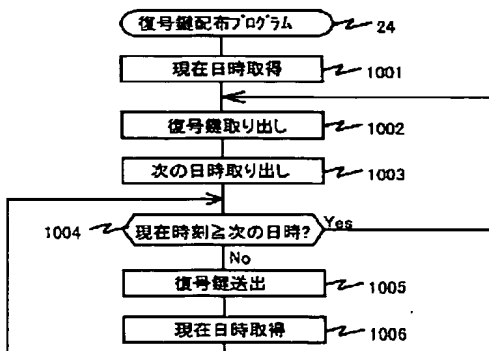
【図11】

図11



【図7】

図7



【図8】

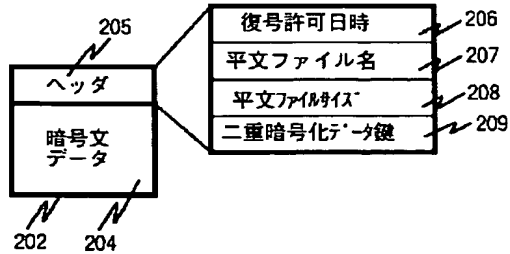
図8

1997/01/01 00:00		199701010000	F7C3B...935B
		199701010000	F7C3B...935B
		199701010000	F7C3B...935B
		...	
1997/01/01 01:00		199701010000	F7C3B...935B
		199701010100	6056D...7E9C
		199701010100	6056D...7E9C
		199701010100	6056D...7E9C
		...	
1997/01/01 02:00		199701010100	6056D...7E9C
		199701010200	413A6...F103
		199701010200	413A6...F103
		199701010200	413A6...F103
		...	

復号鍵公開履歴

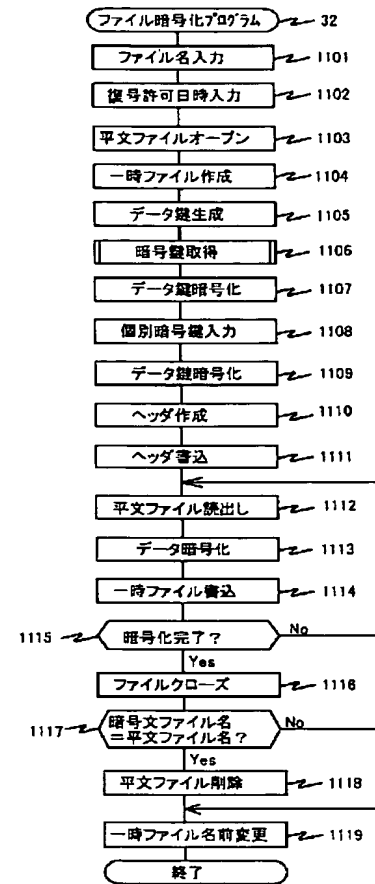
【図9】

図9



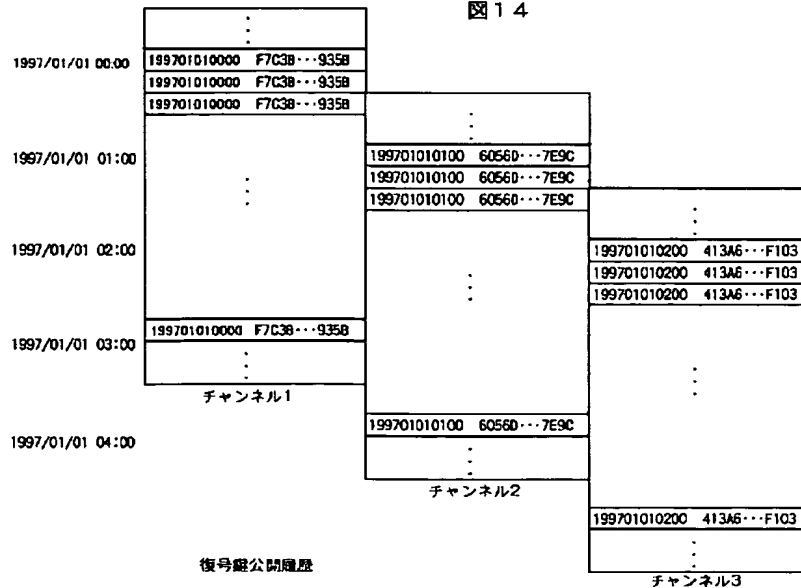
【図10】

図10



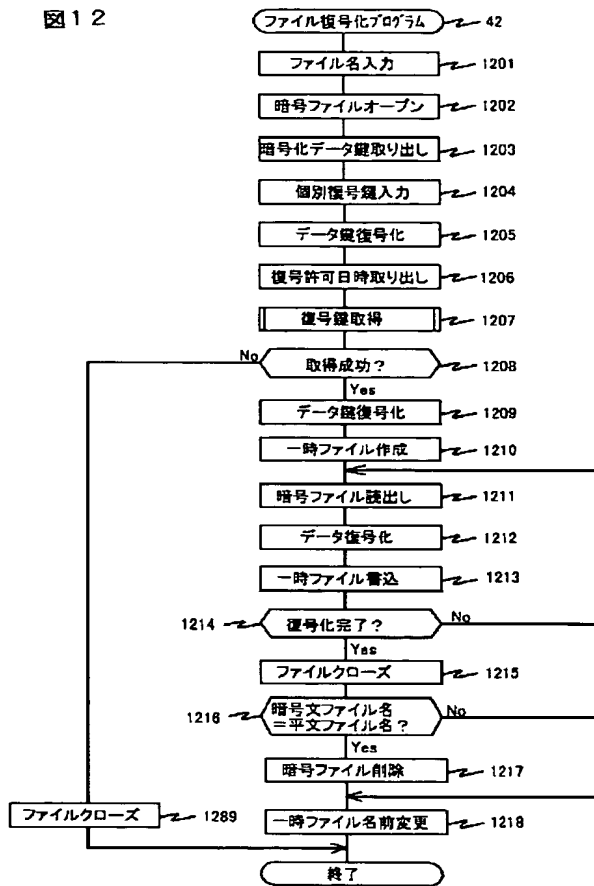
【図14】

図14



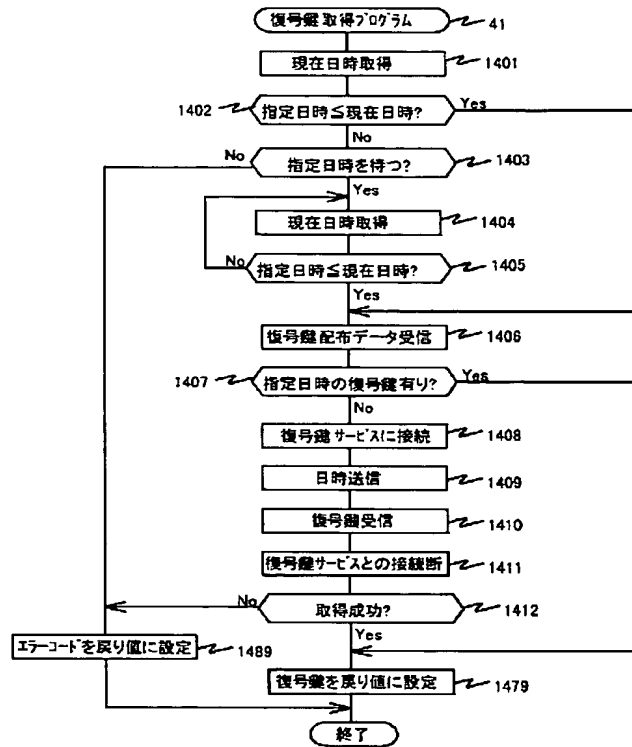
【図 12】

図 12



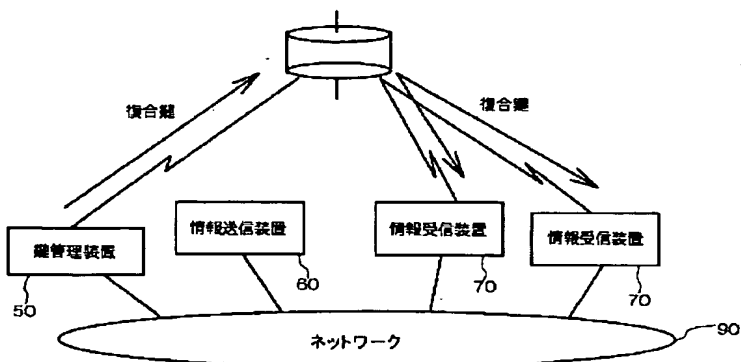
【図 13】

図 13



【図 15】

図 15



フロントページの続き

(51) Int. Cl. ⁷

識別記号

F I

テーマコード(参考)

H O 4 L 9/08

H O 4 L 9/00

6 0 1 F

F ターム(参考) 5B017 AA03 AA06 BA07 BB09 BB10
CA16
5J104 AA16 BA03 EA04 EA16 NA02
NA20 PA07